Oracle Keystores – Der Schlüssel zum Glück

Andreas Chatziantoniou
Foxglove-IT BV
Utrecht, Niederlande

Schlüsselworte

Oracle Keystore, OPSS, Security

Einleitung

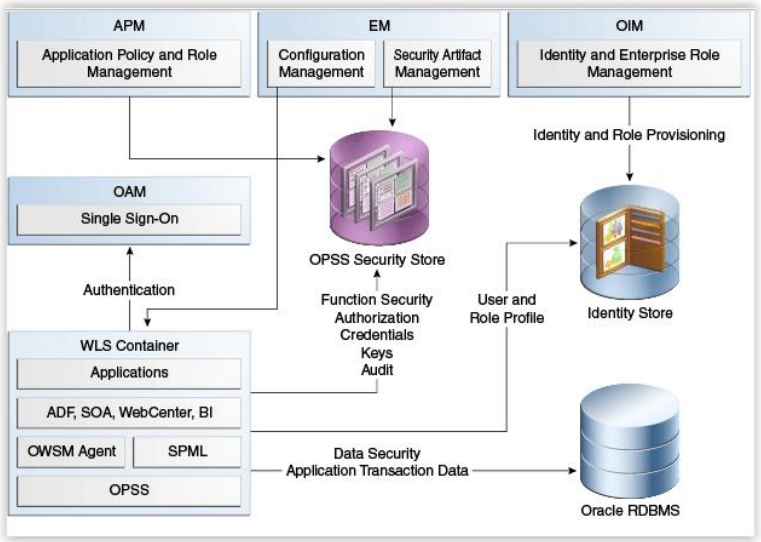
Seit Weblogic 12 gibt es den OPSS Keystore Service (KSS). Dieser Vortrag zeigt an der Hand von Beispielen und einer End-To-End-Einbettung wie die verschiedenen FMW Komponenten mit OPSS und dem KSS arbeiten können. Unterschiede zu den bisherigen JKS werden aufgezeigt.

Oracle Keystores

Seit Anbeginn der IT war Security ein Thema. Betrachtet man die Komponenten eines IT Systems dann ist der Zugang zu den Daten wahrscheinlich der sensibelste Teil auf dem Sicherheitsmechanismen greifen müssen. Denn wer die Daten kontrolliert braucht sich nicht mehr um die verschiedenen Lagen der Zugangskontrolle in den darüber liegenden Schichten zu kümmern. Normalerweise bietet die Oracle Datenbank hier genug Möglichkeiten um die Daten zu schützen. Ob dies nun die normalen Rollen und Rechte auf Tabellen sind, Virtual Private Database, Label Security, Transparent Data Encryption usw. – wir können davon ausgehen, dass unsere Daten nur denen zugänglich sind die diesen Zugang auch haben.

Eine Ebene höher – auf dem Niveau des Application Servers – muss nun ein vergleichbares Konstrukt vorhanden sein, um die Zugangskontrolle zu implementieren.

Die Oracle Keystores sind Teil des OPSS – der Oracle Platform Security Services. Die folgende Zeichnung zeigt deutlich die Position der Oracle Keystores innerhalb des OPSS:



Anlegen des Keystores

Alle Keys des Oracle Keystores werden im zentralen OPSS Security Store abgelegt. Der OPSS Security Store kann hierbei entweder Dateibasiert, LDAP-Basiert oder DB-basiert sein. Dies wird beim Anlegen des OPSS Security Stores festgelegt.

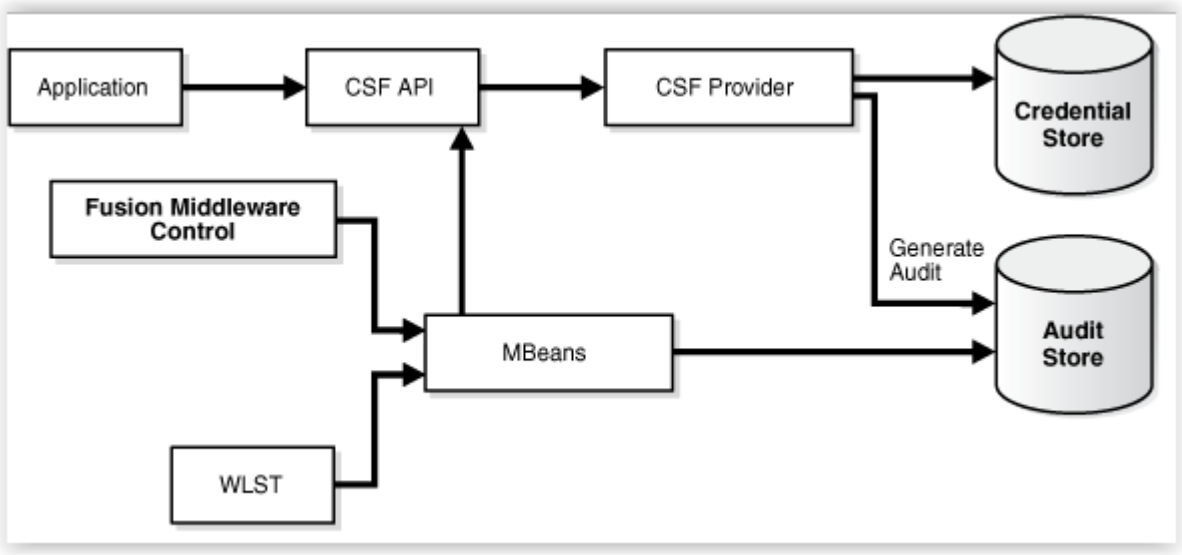
Das Anlegen des OPSS kann mit Hilfe des Repository Creation Utility (RCU), dem Enterprise Manager oder mit Skripten erfolgen.

Unterstützung verschiedener Topologien

Das Konzept des KSS ist darauf ausgelegt um in einfachen Umgebungen zu funktionieren, bietet aber auch die Unterstützung für komplexe Set-ups. Die File-basierte Konfiguration ist sicherlich für Stand-Alone Umgebungen geeignet, läuft aber gegen die Grenze wenn eine Hochverfügbarkeit erfordert ist. Dann sollte der KSS in einem LDAP Server bzw. einer Datenbank abgelegt sein. Diese müssen dann durch geeignete Mittel (LDAP Replikation, DB RAC evt. erweitert mit Data Guard) so eingerichtet werden, damit Multi-Datacenter Set-ups unterstützt werden.

Benutzung durch Anwendungen

Die folgende Zeichnung zeigt wie eine Anwendung über das Credential Store Framework den Credential Store (KSS) benutzt. Hierbei werden durch das CSF die Credentials (Benutzername, Password, Keys, usw.) aus dem Credential Store abgeholt. Wichtig für den sicheren Betrieb der Anwendung ist die gleichzeitige Einbindung des Auditing. Somit kann die korrekte Funktionsweise der Anwendung überwacht werden.



OPSS Security Services sind in den Management Tools der Oracle Fusion Middleware integriert. Hierdurch können die OPSS Security Policies und Konfigurationen mit den bekannten Werkzeugen (z.B. der Fusion Middleware Console, WLST, JMX MBeans) ausgeführt werden.

Lifecycle Management

Der Oracle Keystore Service enthält verschiedene Möglichkeiten zum Lifecycle Management. Dies sind u.a.

- Anlegen des KSS
- Update des KSS
- Löschen des KSS
- Import und Export
- Passwordänderung des KSS

Diese Lifecycle Management Optionen sind im WLST und in der Fusion Middleware Console vorhanden.

Certificate Management

Da die Sicherheit in IT Systemen üblicherweise von Certificates abhängt, bietet der Oracle Keystore Service Unterstützung von Certificate Management an.

Zu den Funktionen gehören:

- Anlegen eines Keypair
- Anlegen eines Certificate Signing Requests
- Import und Export von Certificates
- Löschen eines Certificates

Auch hier sind alle Funktionen von der Fusion Middleware Console oder dem WLST ausführbar.

Weiterhin können auch bestehende Certificates aus einem Java Key Store oder einer Oracle Wallet importiert werden.

„Lokaler KSS“

Wie oben schon angezeigt können Anwendungen die Daten des KSS benutzen indem das CSF genutzt wird. Beim Starten vom WebLogic Server oder einem Nodemanager ist es jedoch notwendig um die Sicherheitsdaten lokal vorrätig zu haben. Hierfür besteht ein WLST Kommando um die KSS Daten lokal abzulegen.

Kontaktadresse:

Andreas Chatziantoniou

Foxglove-IT BV

Texel 18

NL-3524 AP Utrecht

Niederlande

Telefon: +31 6 23 25 91 67

E-Mail andreas@foxglove-it.nl